User's Guide

Acronis Privacy Expert 9.0

Corporate

Acronis

Compute with confidence

www.acronis.com

Copyright © Acronis, Inc., 2000-2006. All rights reserved.

Windows is registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED «AS IS» AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

END-USER LICENSE AGREEMENT

BY ACCEPTING, YOU (ORIGINAL PURCHASER) INDICATE YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT WISH TO ACCEPT THE PRODUCT UNDER THESE TERMS, YOU MAY CHOOSE NOT TO ACCEPT BY SELECTING "I decline..." AND NOT INSTALLING THE SOFTWARE.

The Acronis Privacy Expert Corporate (the software) is Copyright © Acronis, Inc., 2000-2006. All rights are reserved. The ORIGINAL PURCHASER is granted a LICENSE to use the software only, subject to the following restrictions and limitations.

1. The license is to the original purchaser only, and is not transferable without prior written permission from Acronis.
2. The original purchaser may use the software on a single computer owned or leased by the original purchaser. You may not use the software on more than one machine even if you own or lease all of them, without the written consent of Acronis.
3. The original purchaser may not engage in, nor permit third parties to engage in, any of the following:

A. Providing or permitting use of or disclosing the software to third parties.

B. Providing use of the software in a computer service business, network, timesharing or multiple user arrangement to users who are not individually licensed by Acronis.

C. Making alterations or copies of any kind in the software (except as specifically permitted above).

D. Attempting to un-assemble, de-compile or reverse engineer the software in any way.

E. Granting sublicenses, leases or other rights in the software to others.

F. Making copies or verbal or media translations of the users guide.

G. Making telecommunication data transmission of the software.

Acronis has the right to terminate this license if there is a violation of its terms or default by the original purchaser. Upon termination for any reason, all copies of the software must be immediately returned to Acronis, and the original purchaser shall be liable to Acronis for any and all damages suffered as a result of the violation or default.

ENTIRE RISK

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU THE PURCHASER. ACRONIS DOES NOT WARRANT THAT THE SOFTWARE OR ITS FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ANY DEFECTS WILL BE CORRECTED. NO LIABILITY FOR CONSEQUENTIAL DAMAGES — IN NO EVENT SHALL ACRONIS OR ITS VENDORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR THE LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF ACRONIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

END-USER LICENSE AGREEMENT 3

INTRODUCTION 6

What is Acronis Privacy Expert Corporate? 6
Acronis Privacy Expert Corporate key features 6
Acronis Privacy Expert Corporate Architecture 7
What's new in Acronis Privacy Expert 9.0 Corporate? 7
Software use conditions 8
Technical support 8

CHAPTER 1. INSTALLING ACRONIS PRIVACY EXPERT CORPORATE COMPONENTS 9

1.1 System requirements 9
1.2 Supported operating systems 9
1.3 Setting up security parameters for Acronis Privacy Expert Corporate 9
1.3.1 Usernames and passwords 9
1.3.2 Firewall setup 10
1.4 License policy 10
1.5 Installing Acronis Privacy Expert Corporate components onto a current computer 10
1.6 Extracting Acronis Privacy Expert Corporate components 11
1.7 Installing Acronis components onto remote machines 11
1.8 Upgrading Acronis Privacy Expert Corporate 13
1.9 Recovering Acronis Privacy Expert Corporate 13
1.10 Removing Acronis Privacy Expert Corporate 13

CHAPTER 2. USING ACRONIS PRIVACY EXPERT CORPORATE MANAGEMENT CONSOLE 14

2.1 Getting started 14
2.2 Acronis Privacy Expert Corporate Management Console main window 14
2.3 Connecting to remote computer 15
2.3.1 Automatic connection 15
2.3.2 Manual connection 15

CHAPTER 3. MALWARE REMOVAL FROM NETWORK COMPUTERS 16

3.1 How malware gets on user's PC 16
3.2 How to recognize malware? 16
3.3 Malware removal 17
3.3.1 Running Malware Removal Wizard 17
3.3.2 Selecting remote computers for malware removal 17
3.3.3 Selecting scanning mode 18
3.3.4 Enabling reboot of remote computers and the task summary 19
3.4 Scheduling malware removal group tasks 19
3.4.1 Selecting remote computers 19
3.4.2 Selecting task and malware scan mode 20
3.4.3 Scheduled tasks preferences 20
3.4.4 Entering user name and password 21
3.4.5 Enabling reboot of remote computers and the task summary 22
3.5 Cancelling and deleting tasks for remote computers 22
3.6 Quarantine 22
3.6.1 Restoring deleted objects 23
3.6.2 Clearing deleted objects 24
3.7 Using the Log 24

CHAPTER 4. USING ACRONIS MALWARE SHIELD 26

4.1 Enabling Acronis Malware Shield 26

Copyright © Acronis, Inc., 2000-2006

4.2 Setting up Malware Shield ... 27
4.2.1 Setting up the system protection level ... 27
4.2.2 General settings ... 28
4.2.3 Process analyzing ... 29
4.2.4 Registry protection ... 29
4.2.5 Process protection ... 30
4.2.6 Files protection ... 31
4.2.7 Specified rules ... 31
4.2.8 History ... 32
4.2.9 Saving settings for Acronis Malware Shield ... 32
4.3 Handling the Malware Shield Alerts ... 32

CHAPTER 5. MALWARE DEFINITIONS UPDATES ... 34

5.1 Malware database update ... 34
5.1.1 Running Malware Definitions Updates Wizard ... 34
5.1.2 Selecting remote computers to update malware definitions ... 34
5.1.3 Selecting update mode ... 35
5.1.4 Setting the schedule ... 35
5.1.5 Entering user name and password ... 36

CHAPTER 6. ACRONIS POP-UP BLOCKER ... 37

6.1 What are pop-ups? ... 37
6.2 Acronis Pop-up Blocker ... 37
6.3 Acronis Pop-up Blocker options ... 37
6.3.1 Acronis Pop-up Blocker General Settings ... 37
6.3.2 User List ... 38
6.3.3 Black List ... 39
6.3.4 History ... 40
6.3.5 Acronis Pop-up Blocker options ... 41

APPENDIX A. MALWARE THREATS GLOSSARY ... 43

Adware ... 43
Backdoors ... 43
Browser Helper Objects ... 43
Browser hijackers ... 43
Commercial keylogger ... 43
Dialers ... 43
Exploit/Security holes ... 44
Remote Administration ... 44
Rootkits ... 44
Sniffers ... 44
Spyware ... 44
Toolbars ... 44
Trojan Horses (Trojans) ... 45

Copyright © Acronis, Inc., 2000-2006

Introduction

What is Acronis Privacy Expert Corporate?

Malware (malicious software), a technology that aids crooks and others gather information about a person or organization without their knowledge, is becoming a huge threat to business networks. It can **leak valuable, confidential information about your organization** to outside entities and can ultimately slow down network performance, impacting your employees' productivity. IT managers recognize malware's potential negative impact. According to a January 2005 survey, two thirds of IT managers think that malware is the number one security **threat to their networks**.

Acronis has a solution to **ensure that malware will not be a threat to your organization or corporate network**. The Acronis Privacy Expert Corporate is a comprehensive anti-malware solution that **proactively protects** your organization from malware programs that can expose confidential information and diminish PC performance.

Acronis Privacy Expert Corporate is **more than just an anti-malware solution.** It also includes Acronis Pop-up Blocker - a **value-added tool** ensuring free of most annoying advertisement Internet navigation.

Acronis Privacy Expert Corporate key features

- **Remote deleting of malware programs** from network computers to ensure that outside entities do not obtain access to internal/confidential data
    - Managing malware tasks on networked computers from one central location
    - Scheduling malware scans on all networked computers on a regular basis without user intervention
    - Smart scanning searches for malware in the most likely locations, including system, user profile and temporary files folders, as well as in the system registry
    - Deep scanning searches all folders on the PC hard drive
    - Keylogging detection protects usernames and passwords from getting into outside hands
    - Quarantine feature enables the administrator to look through the list of the objects (files, registry keys etc.), deleted by malware removal operations, and restore any of them, in the unlikely case it would be useful
- **Remote installation** of Acronis Privacy Expert Corporate components to network computers

 Copyright © Acronis, Inc., 2000-2006

- **Comprehensive Malware Shield** prevents malware from being installed to networked computers
    - Constantly monitors running processes and provides alerts due to any suspicious actions of programs, such as trying to change the Windows registry and to launch at startup
    - Prevents the changing of settings of ActiveX components
    - Prevents applications from making changes to Web browser settings, including home page, search page, etc. This ensures that employees go to the pages they select
- **Pop-up ad blocker** ensures that annoying pop-up ads do not interfere with Web browsing
- **Internet updates** service keeps malware definitions up-to-date. Updates can be downloaded manually via a wizard or automatically downloaded as a scheduled task

Acronis Privacy Expert Corporate Architecture

Acronis Privacy Expert Corporate includes the following components:

1. Acronis Privacy Expert Corporate Management Console — helps you install and manage the Acronis Privacy Expert Corporate Agent on a remote machine; removes malware threats on the remote computers, schedules malware removal tasks, browses logs and more

2. Acronis Privacy Expert Corporate Agent — installs on a remote system to enable access from the Acronis Privacy Expert Corporate Management Console

3. Acronis Malware Shield — installs on a remote computers and monitors it for suspicious applications and components

4. **Acronis Pop-up Blocker -** installs on a remote computers and blocks unwanted pop-up windows there.

What's new in Acronis Privacy Expert 9.0 Corporate?

- Enhanced **malicious software removal engine** includes rootkit detection and removal feature
- Enhanced **Malware Shield** allows setting the level of your system proactive protection (high, medium, or low)
- **Daily** malware definition updates
- Enhanced **Malware Quarantine Wizard**
- Enhanced **Pop-up Blocker** allows setting the protection level (high, medium, or low) and selection of the type of the content being blocked.

Additional improvements have been made to provide even more convenience for users.

Copyright © Acronis, Inc., 2000-2006

Software use conditions

The conditions for Acronis Privacy Expert Corporate software usage are described in the «License Agreement» (page 3 of this manual). A set of unique serial keys, supplied with the product, is the confirmation of the legal purchase and usage the suite.

Under current legislation, the «License Agreement» is considered a contract between the user and software vendor. The contract is a legal document and its violation may result in legal action.

Illegal use and/or distribution of this software will be prosecuted

Technical support

Users of legally purchased copies of Acronis Privacy Expert Corporate are entitled to free technical support from Acronis. If you experience problems installing or using Acronis products that you can't solve yourself by using this guide, then please contact Acronis Technical Support.

More information about contacting Acronis Technical Support is available at the following link: http://www.acronis.com/enterprise/support/

Copyright © Acronis, Inc., 2000-2006

Chapter 1. Installing Acronis Privacy Expert Corporate components

1.1 System requirements

To take full advantage of Acronis Privacy Expert Corporate, you should have:

- a PC-compatible computer with a Pentium CPU or equivalent
- 256 MB RAM
- a floppy or a CD-RW drive
- a mouse (recommended)
- Microsoft Internet Explorer 4.0 or higher for correct Pop-up Blocker operation

1.2 Supported operating systems

For all Acronis Privacy Expert Corporate components:

- MS Windows 98/Me
- MS NT 4.0 Workstation Service Pack 6 / 2000 Professional / XP
- MS NT 4.0 Server Service Pack 6 / 2000 Server / 2000 Advanced Server, 2003 Server.

1.3 Setting up security parameters for Acronis Privacy Expert Corporate

1.3.1 Usernames and passwords

Acronis Privacy Expert Corporate fully supports all security standards used in Windows:

1. If a remote PC has Windows NT/2000/XP OS installed, the Acronis Privacy Expert Corporate Agent can be accessed according to the security policy set up in the local network. To have remote access to Acronis Privacy Expert Corporate Agent, the user must be a member of the **Administrators** group on this computer.

It is highly recommended that you create an administrator's account with the same username and password on all networked computers for remote access to the Acronis Privacy Expert Corporate Agent.

2. If a remote PC has Windows 98/Me installed without its own security system, you will need to provide a username and password during installation of the Acronis Privacy Expert Corporate Agent that will be used by Acronis Privacy Expert Corporate Management Console.

Copyright © Acronis, Inc., 2000-2006

1.3.2 Firewall setup

Acronis Privacy Expert Corporate uses the following ports and IP addresses for remote operation:

- **SERVER (ACRONIS PRIVACY EXPERT CORPORATE AGENT) UDP PORT:** 9876
- **SERVER (ACRONIS PRIVACY EXPERT CORPORATE AGENT) TCP PORT:** 9876, IF BUSY CHOSE PORT AT RANDOM
- **CLIENT (ACRONIS PRIVACY EXPERT CORPORATE MANAGEMENT CONSOLE) UDP PORT:** 9877, IF BUSY CHOSE PORT AT RANDOM
- **IPV4 MULTICAST ADDRESS:** 239.255.219.45
- **IPV6 MULTICAST ADDRESS:** FF05::FAA5:741E

You might have to set the appropriate firewall access options. Options for the Windows Firewall, included in Windows XP Service Pack 2 are set automatically during Acronis Privacy Expert Corporate components installation. However, make sure that the option **File and Printer Sharing** in the **Control panel** → **Windows Firewall** → **Exceptions** is enabled on the remote computer before the remote operation starts.

1.4 License policy

Acronis Privacy Expert Corporate licensing is based on the number of computers on which the **Acronis Privacy Expert Corporate Agent, Acronis Malware Shield,** or **Acronis Pop-up Blocker** are to be installed. The number of **Acronis Privacy Expert Corporate Management Console** installations is not counted.

1.5 Installing Acronis Privacy Expert Corporate components onto a current computer

Run Acronis Privacy Expert Corporate setup file. In the Install Menu, select the component that you are going to install on a current PC: Acronis Privacy Expert Corporate Management Console, Acronis Privacy Expert Corporate Agent, Acronis Malware Shield, or Acronis Pop-up Blocker. Follow instructions shown in the installation wizard.

If your version of Acronis Privacy Expert Corporate uses Acronis License Server, you should install Acronis License Server and import the serial keys before installing the licensed Acronis Privacy Expert Corporate components. For more information see Acronis License Server User's Guide.

 Copyright © Acronis, Inc., 2000-2006

Acronis Privacy Expert Corporate installation window

MS Installer version 2.0 or newer is required. If the setup program does not find this utility on your computer, it prompts to install MS Installer 2.0, included into Acronis Privacy Expert Corporate pack. Choose **Yes** in the appearing dialog box.

If you are installing Acronis Pop-up Blocker on the computer with MS Windows 2003 Server operating system be sure that registry key value for `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Enable Browser Extensions` was sets as **Yes**.

After installation is completed, you may be prompted to restart the computer.

1.6 Extracting Acronis Privacy Expert Corporate components

You may want to save setup (.msi) files for each Acronis Privacy Expert Corporate component separately on a local or network drive. Then you will be able to install the components in the command-line mode using msiexec.exe utility. It also will help to modify or recover the existing component installation.

To save a setup file:

- run the Acronis Privacy Expert Corporate setup file;
- in the Install Menu, right-click on the component name and select **Extract**;
- select location for setup file and click **Save**.

1.7 Installing Acronis components onto remote machines

Acronis Privacy Expert Corporate Management Console allows you to install Acronis components onto remote computers, connected to the corporate network.

Using the Acronis Privacy Expert Corporate Management Console, you can install remotely:

- Acronis Privacy Expert Corporate Agent

Copyright © Acronis, Inc., 2000-2006

- Acronis Malware Shield
- Acronis Pop-up Blocker

To install any Acronis component to a remote machine, you will need administrator rights on the target machine.

You can remotely install Acronis components only onto machines working under Windows NT/2000/XP (including server versions). Windows 98/Me machines will require local installation of Acronis components.

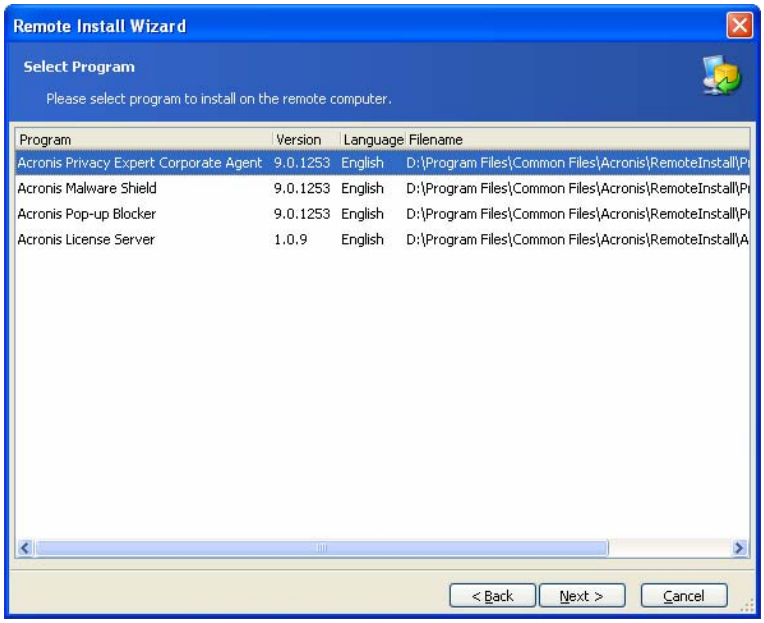
If the remote PC runs under Windows XP, make sure the option **Use simple file sharing** in the **Control panel → Folder options → View** is disabled before the remote installation starts.

If the remote PC runs under Windows XP with Service Pack 2 installed, make sure that the option **File and Printer Sharing** in the **Control panel → Windows Firewall → Exceptions** is enabled before the remote installation starts.

If your version of Acronis Privacy Expert Corporate uses Acronis License Server, you should install Acronis License Server and import the serial keys before installing the licensed Acronis Privacy Expert Corporate components. For more information see Acronis License Server User's Guide.

To install Acronis components:

- Select the **Install Acronis components** button on the Toolbar or select **Tools → Install Acronis components** from the main menu
- Select the Acronis components you want to install (Acronis Privacy Expert Corporate Agent, Acronis Malware Shield or Acronis Pop-up Blocker)



- In the next window, select the remote computers on which the Acronis components are to be installed
- Enter the program serial key or specify the license server, depending on the product version

Copyright © Acronis, Inc., 2000-2006

- The Acronis components then will be installed to the remote computers you specified
- If you checked **Reboot the remote computer(s)** box during the component installation, the remote machines will reboot. Otherwise, you will see the corresponding message.

1.8 Upgrading Acronis Privacy Expert Corporate

If you have any previous version of Acronis Privacy Expert Corporate installed, you must uninstall all its components, including Acronis License Server, either locally from Windows **Control Panel -> Add and Remove Program**, or remotely, using Acronis Privacy Expert Corporate Management Console, and after that run Acronis Privacy Expert 9.0 Corporate installation procedure.

If you try to remotely install a new product version over the old one, the Console will suggest to uninstall the old version. If you do not agree, you will not be able to install the new version.

Every customer who has purchased Acronis Privacy Expert 8.0 Corporate is eligible for free upgrade to the 9.0 version.

1.9 Recovering Acronis Privacy Expert Corporate

You can reinstall Acronis Privacy Expert Corporate components if nesessary. To do this, launch the installation program again.

The installer will determine that the component has already been installed to the computer and ask if you want to **Modify, Repair** or **Remove** it from the disk.

Select **Repair** Acronis Privacy Expert Corporate and click **Next**. All files will be copied to your hard disk again to restore the program.

To repair Acronis Privacy Expert Corporate components installed on remote computers, reinstall them as described in *1.7*.

1.10 Removing Acronis Privacy Expert Corporate

You can remove any Acronis Privacy Expert Corporate component separately by selecting **Control panel → Add or remove programs → <The component name> → Remove.** Then follow the instructions on the screen.

Copyright © Acronis, Inc., 2000-2006

Chapter 2. Using Acronis Privacy Expert Corporate Management Console

2.1 Getting started

Acronis Privacy Expert Corporate Management Console is the primary tool for managing Acronis components on remote computers with the Acronis Privacy Expert Corporate Agent installed.

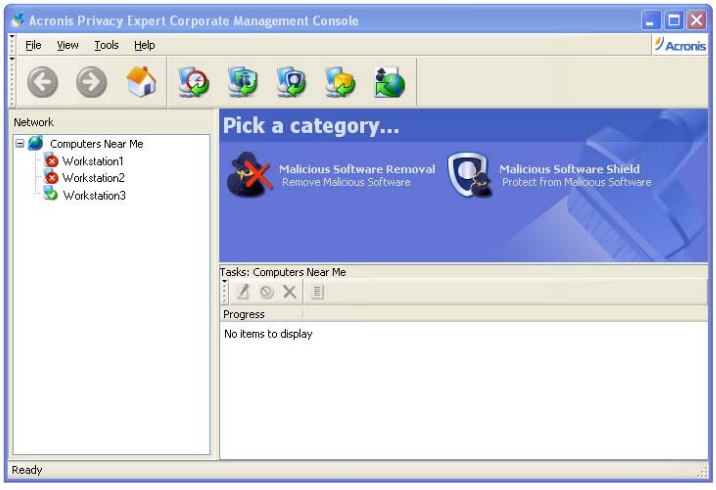
Acronis Privacy Expert Corporate Management Console is launched by selecting **Start → All programs → Acronis → PrivacyExpert → Acronis Privacy Expert Corporate Management Console** or double-clicking the respective desktop shortcut.

With the Acronis Privacy Expert Corporate Management Console, you can:

- Install Acronis components to remote computers
- Remove malware and malicious programs from the remote computers (workstations)
- Turn off/on Acronis Malware Shield on remote computers
- Browse logs of Acronis Privacy Expert Corporate operations
- Browse the remote computers' Quarantines and restore any of deleted objects (files, registry keys etc.), if necessary

2.2 Acronis Privacy Expert Corporate Management Console main window

The Acronis Privacy Expert Corporate Management Console main window contains three areas:



Copyright © Acronis, Inc., 2000-2006

Acronis Privacy Expert Corporate Management Console main window

- **Operations categories,** where you can select operations to perform on the remote computers (**Malware Removal** or **Malware Shield** setting up).

  To move between categories or return to the main window use **Back**, **Next** and **Other categories** buttons on the toolbar.

- **Network** panel contains the list of network computers on which Acronis Privacy Expert Corporate Agent is installed.
- **Tasks** panel displays tasks status for the connected remote computer, selected in the **Network** panel. For the task currently running, a progress bar is displayed. The **Task** panel has its own toolbar with **Show log** button, viewing reports on remote operations for each computer, **Delete** button to delete scheduled tasks, and **Cancel** button to interrupt the currently running tasks.

2.3 Connecting to remote computer

To perform any operation on a remote computer, you must first connect to it.

2.3.1 Automatic connection

Acronis Privacy Expert Corporate Management Console automatically connects at startup to all computers running Acronis Privacy Expert Corporate Agent and having the same user account as that of the user who runs the Console. If you create an administrator's account with the same username and password on all networked computers and run Acronis Privacy Expert Corporate Management Console having logged on with this account profile, all computers will automatically connect at the Console startup.

2.3.2 Manual connection

To connect to a computer that does not have the unified account, right-click on the computer name in the **Network** panel and choose **Connect.** In the Remote Connection Wizard windows, check the computer (or several computers) you would like to connect and enter user name and password to access to this computer(s).

Copyright © Acronis, Inc., 2000-2006

Chapter 3. Malware removal from network computers

There are many programs that, once on user's PCs, start working without user's knowledge. Such software can do such things as collect information or change user settings for the Internet or your system. These programs are called **malware**. For more information on the main malware types, see **Appendix A** of this guide.

Acronis Privacy Expert Corporate enables you to completely clean user's computers of malware and protect it from future intrusions.

3.1 How malware gets on user's PC

One of the most common ways that malware gets on a user's PC is from new software installations. This is particularly true with freeware and shareware. When user installs such applications, they can implement software modules that collect information on Web sites user visits, user's PC configuration, and other sources.

Other common sources of malware include peer-to-peer networks, gaming portals and other similar Web services.

Sometimes malware is installed by commercial applications whose makers want to collect additional information about users, their habits and preferences.

3.2 How to recognize malware?

Though in many cases malware works without users' knowledge, there are signs that you should watch for:

- Hard drives LEDs are blinking even when no programs are running or documents are open
- User's PC receives and sends unknown information via the Internet, even though the Web browser and e-mail client are not active
- The home page setting of the Internet browser has changed without the user's consent
- The user sees ads or pop-ups while running programs or visiting Web sites

If you notice any or all of these activities on your users' computers, you need to run Acronis Privacy Expert Corporate to find and eliminate malware performing unauthorized operations on the workstations.

 Copyright © Acronis, Inc., 2000-2006

If you need to:

- Find and remove any type of malware from remote PCs, run **Malware removal**
- Prevent malware from getting on network PCs, enable and set up **Malware Shield** (see *Chapter 4 Using Acronis Malware Shield*).

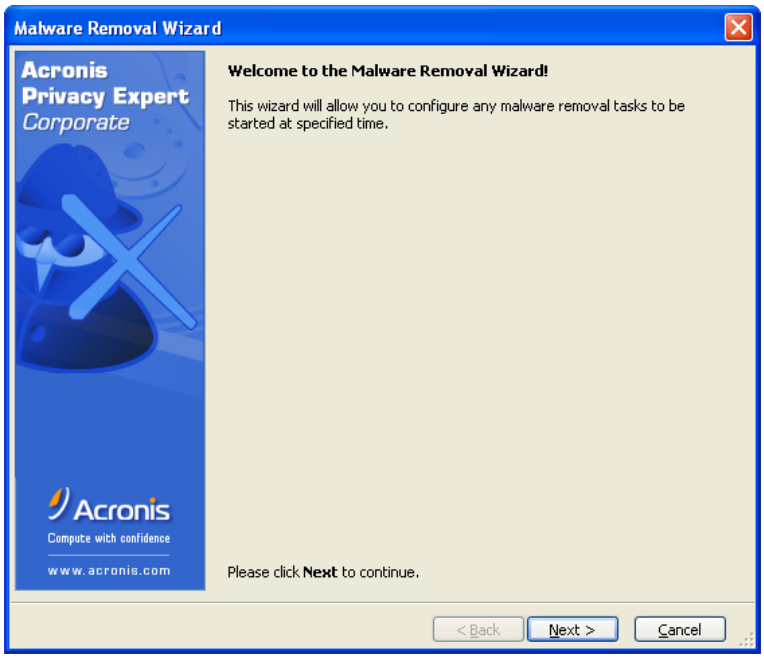
3.3 Malware removal

Using Acronis Privacy Expert Corporate, you can find and remove malware from remote computers in your local network. To do this, select and click **Malicious software removal** in the main program window.

After that, you can either **Remove Malicious Software Now**, or **Update Malicious Software definitions** (see *Chapter 5 Malware definitions updates*).

3.3.1 Running Malware Removal Wizard

To run the **Malware Removal Wizard,** select **Remove Malware Now** in the **Malware Removal** window.

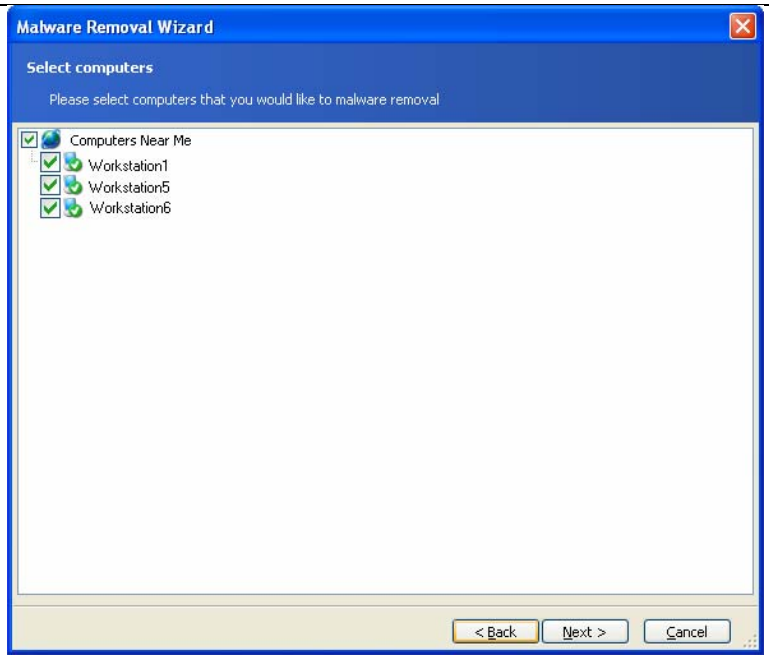


Malware Removal Wizard

3.3.2 Selecting remote computers for malware removal

Next select the remote computers on which you are going to remove malicious programs.

Copyright © Acronis, Inc., 2000-2006

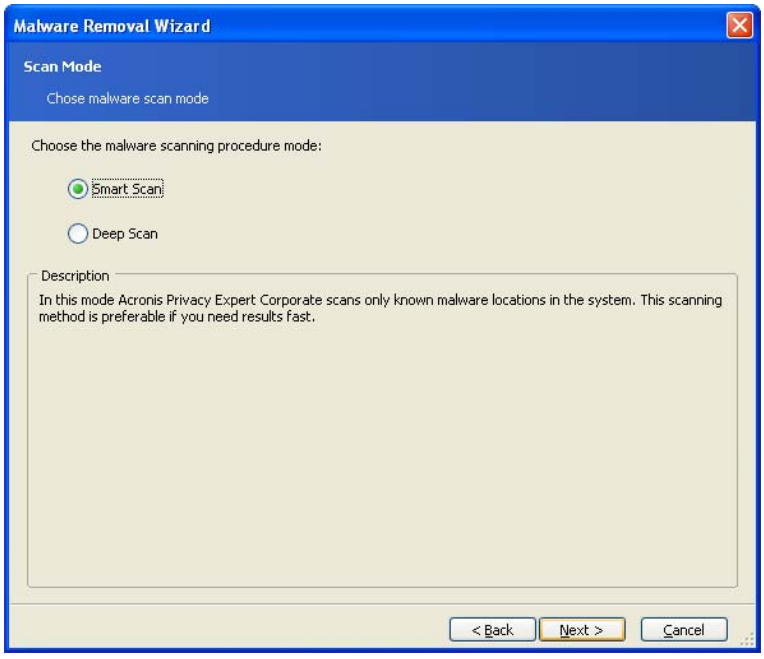


Select computers window

3.3.3 Selecting scanning mode

There are two modes of malware search. Select which one you want to perform:

- **Smart scanning mode** – used by default. The Smart Scanning Mode suite searches for malware only in the most likely locations, including system, user profile and temporary files folders, as well as in the system registry. Select this mode for a quick check.
- **Deep Scanning Mode** – an extended algorithm for malware scanning. In this mode, all folders on all hard drives are searched for malware. This variant could take much more time depending on the capacity of your hard disks.


Malware Removal Wizard
Scan Mode
Chose malware scan mode
Choose the malware scanning procedure mode:
Smart Scan
Deep Scan
Description
In this mode Acronis Privacy Expert Corporate scans only known malware locations in the system. This scanning method is preferable if you need results fast.
< Back
Next >
Cancel

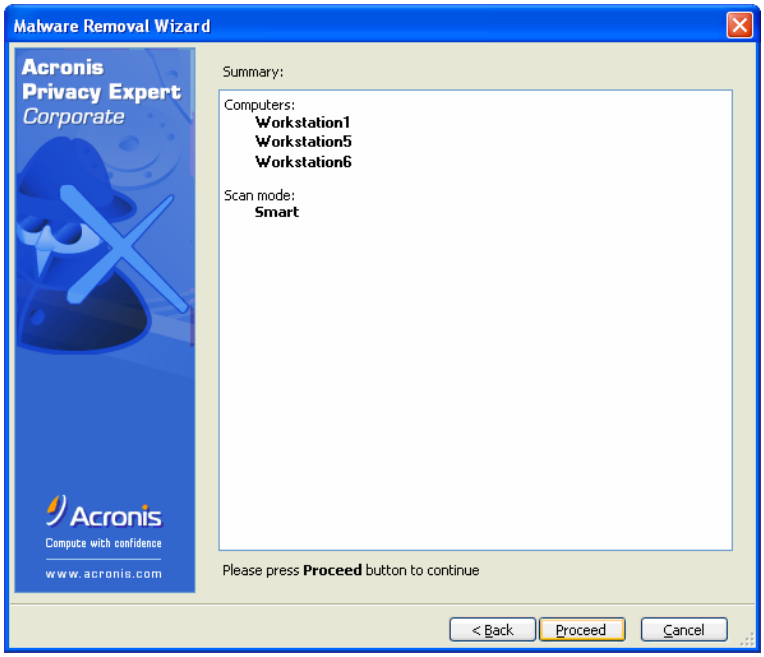
Malware scanning modes

Copyright © Acronis, Inc., 2000-2006

3.3.4 Enabling reboot of remote computers and the task summary

In the next to last Wizard window you can allow reboot of remote computers after malware removal.

The final window displays a preview of the malware removal: a list of remote computers on which this action will be performed, and the malware scan mode – smart or deep.



Malware removal operations summary

To start executing operations, click **Proceed**.

After the malware removal operation is finished, you can see logs for each remote computer with a summary that will state the number of malware applications removed (see section *3.7 Using the Log*).

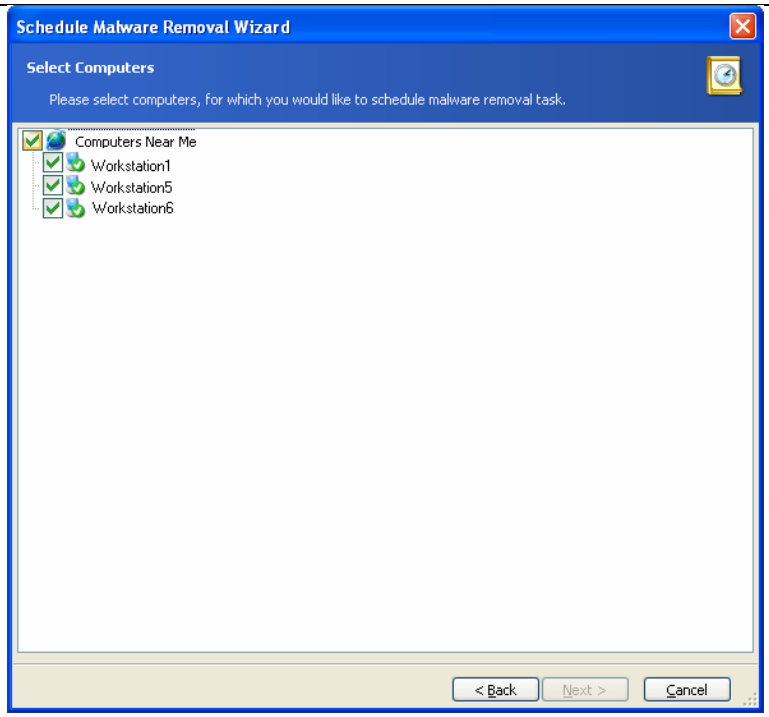
3.4 Scheduling malware removal group tasks

To set up the malware removal schedule for remote computers, click the **Schedule task** button on the toolbar of the Acronis Privacy Expert Corporate Management Console main window or select **Tools** → **Schedule task** section in the main menu.

3.4.1 Selecting remote computers

First, select remote computers on which you want to schedule the task.

Copyright © Acronis, Inc., 2000-2006



Select computers window

3.4.2 Selecting task and malware scan mode

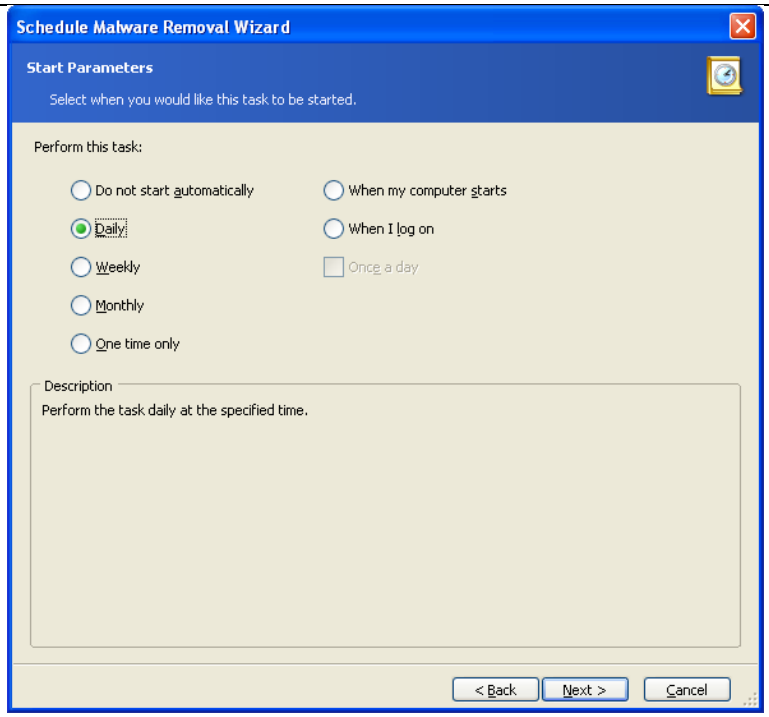
Now select the task to schedule (malware removal) and scan mode (see section *3.3.3 Selecting scanning mode* of this Guide).

3.4.3 Scheduled tasks preferences

Set the task execution periodicity:

- **Do not start automatically**
- **Daily**, according to the schedule with the ability to select only workdays or once every few days
- **Weekly**, according to the schedule with the ability to select particular days, say, Tuesday and Friday, or once every two or three weeks, etc
- **Monthly,** according to the schedule on the time and day set; The suite supports clean-up on the <first, second, third, fourth, last> <day of the week> (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday), for example
- **One time only,** at a specific time (hours:minutes) on a particular day (month/day/year)
- **When my computer starts** (you may specify launching the task once a day only)
- **When I log on** (you may specify launching the task once a day only)

 Copyright © Acronis, Inc., 2000-2006

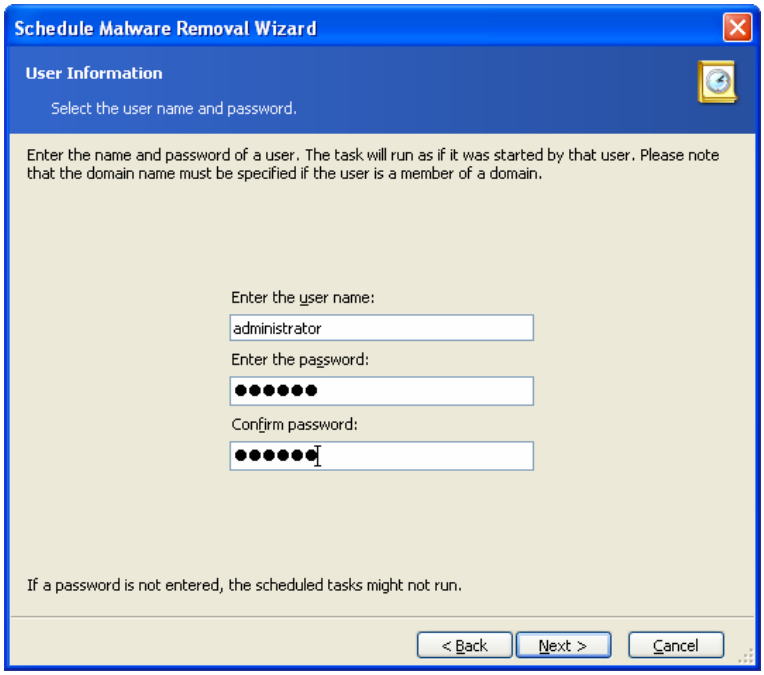


Scheduler set up window

Having made your selection, click **Next** to set additional parameters on the next wizard page.

3.4.4 Entering user name and password

For the remote computers, running Windows NT, 2000, XP or 2003 Server, you will have to specify the name of the user that owns the executed task; otherwise, no scheduled execution would be available.


Schedule Malware Removal Wizard
User Information
Select the user name and password.
Enter the name and password of a user. The task will run as if it was started by that user. Please note that the domain name must be specified if the user is a member of a domain.
Enter the user name:
administrator
Enter the password:
Confirm password:
If a password is not entered, the scheduled tasks might not run.
< Back
Next >
Cancel

Copyright © Acronis, Inc., 2000-2006

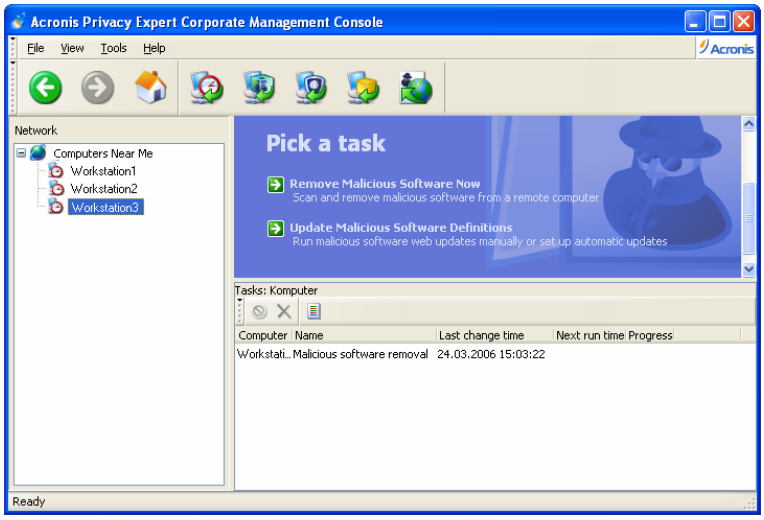
In the upper field, enter a user name. Enter a password twice in two fields below. It is assumed that administrator's accounts with the same username and password exist on all selected computers. The task will not start on computers that do not accept the specified user name and password.

3.4.5 Enabling reboot of remote computers and the task summary

In the next to last Wizard window you can allow reboot of remote computers after malware removal.

You have finished scheduling a task. The wizard will again remind you of the details of the task provided.

After the task is distributed to selected computers, you can see it in the **Tasks** panel of the Acronis Privacy Expert Corporate Management Console. Icons of the computers for which a malware removal task was scheduled, feature a clock image.



3.5 Editing, canceling and deleting tasks for remote computers

You can delete a scheduled malware removal task from any connected computer by selecting the **Delete** button on the **Tasks** toolbar or interrupt executing of a task by clicking the **Cancel** button. To delete the currently running task, first cancel in and then delete.

Also you can edit the scheduled task. To do it select the task and press **Edit tasks** button in the taskbar of the **Tasks** window.

3.6 Quarantine

Though the case is unlikely, you may need to restore some objects (files, registry keys etc.), deleted by malware removal operations. Such might be the case if the system works unstable as a result of malware removal. Besides, it may be useful to look through the list of deleted objects and obtain the detailed

 Copyright © Acronis, Inc., 2000-2006

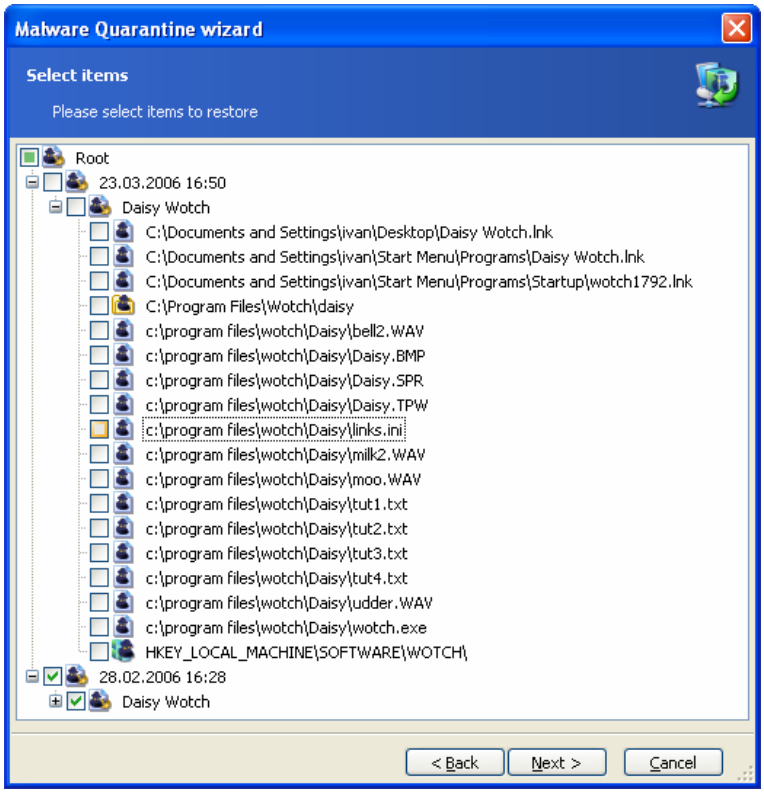
information about Acronis Privacy Expert Corporate operation on remote computers. To allow viewing and recovery of the deleted objects, they are not lost forever, but stored on the user's computer in a special folder, referred to as the Quarantine.

To open the Quarantine on a remote computer, click the **Malware Quarantine** button on the Toolbar or select **Tools** → **Malware Quarantine** from the main menu. Then select a connected remote computer. (You can select only one computer at a time. To list other Quarantines, click **Back** after seeing the current one and select the next computer.)

Next, choose the prospective action (**Restore** or **Clear**) to be taken about the objects in the Quarantine.

3.6.1 Restoring deleted objects

If you select **Restore**, the program displays a list of malware objects, deleted from the selected computer, sorted by date. Check objects to be recovered. Then click **Next** to perform the selected action.

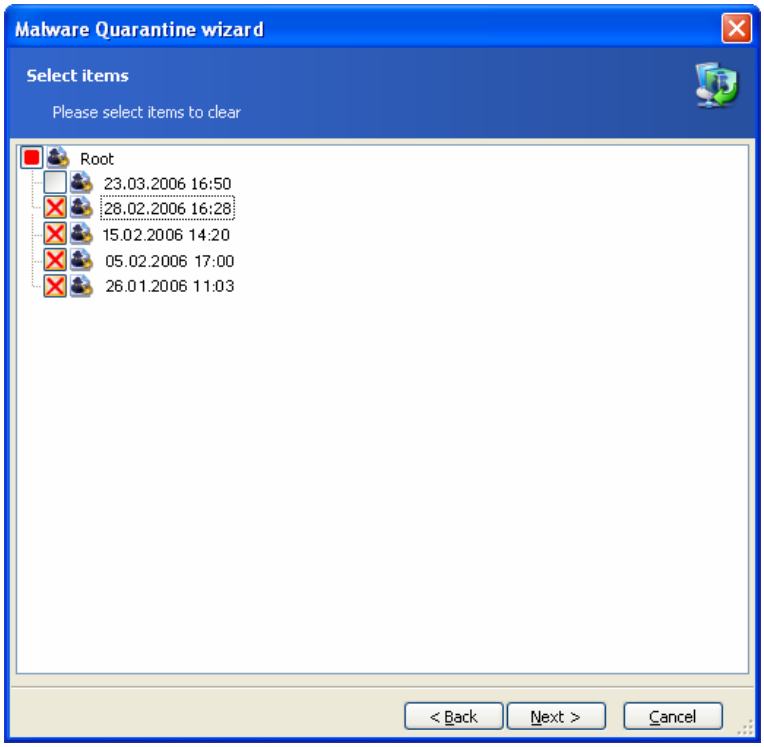


If the system configuration has been changed since the restored objects were placed to the Quarantine, these objects may be inconsistent with the new system configuration. Therefore, it is recommended that you think twice and use restoration feature in a short time after malicious software removal.

Copyright © Acronis, Inc., 2000-2006

3.6.2 Clearing deleted objects

Having chosen **Clear**, you can see only dates when the objects were put to the Quarantine. Select objects to be killed by date. Then click **Next** to perform the selected action.



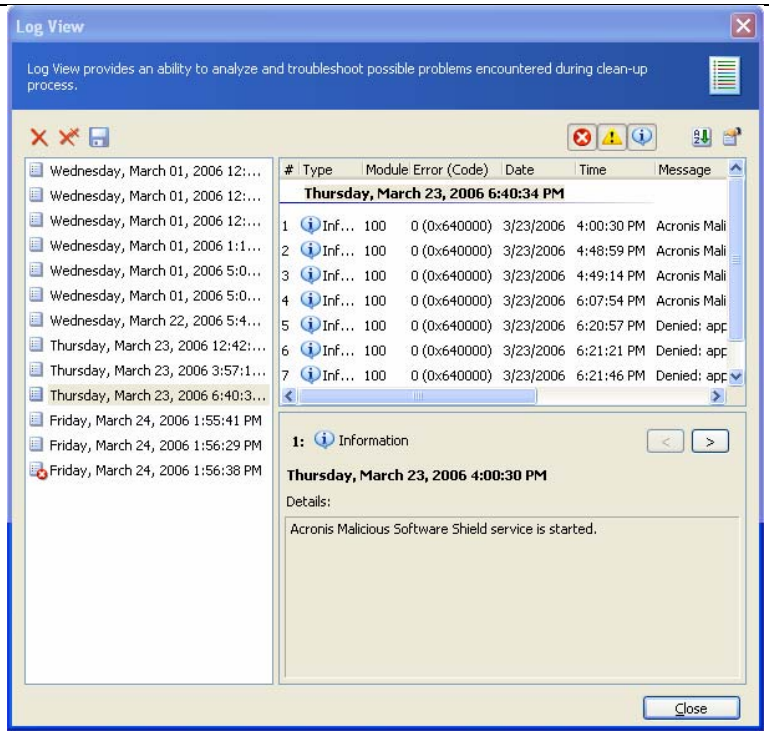
3.7 Using the Log

The **Log** keeps track of all actions performed by Acronis Privacy Expert Corporate on remote computers. It provides a complete history of activities and reasons for any problems that have occurred.

To view logs:

- Select a computer name from the list in the **Network** panel of the Acronis Privacy Expert Corporate Management Console main window
- Left-click on the **Show log** button in the **Task** panel of the Acronis Privacy Expert Corporate Management Console main window
- You will now see logs for the selected computer.

Copyright © Acronis, Inc., 2000-2006


Log View
Log View provides an ability to analyze and troubleshoot possible problems encountered during clean-up process.
Wednesday, March 01, 2006 12:...
Wednesday, March 01, 2006 12:...
Wednesday, March 01, 2006 12:...
Wednesday, March 01, 2006 1:1...
Wednesday, March 01, 2006 5:0...
Wednesday, March 01, 2006 5:0...
Wednesday, March 22, 2006 5:4...
Thursday, March 23, 2006 12:42:...
Thursday, March 23, 2006 3:57:1...
Thursday, March 23, 2006 6:40:3...
Friday, March 24, 2006 1:55:41 PM
Friday, March 24, 2006 1:56:29 PM
Friday, March 24, 2006 1:56:38 PM
Type Module Error (Code) Date Time Message
Thursday, March 23, 2006 6:40:34 PM
1 Inf... 100 0 (0x640000) 3/23/2006 4:00:30 PM Acronis Mali
2 Inf... 100 0 (0x640000) 3/23/2006 4:48:59 PM Acronis Mali
3 Inf... 100 0 (0x640000) 3/23/2006 4:49:14 PM Acronis Mali
4 Inf... 100 0 (0x640000) 3/23/2006 6:07:54 PM Acronis Mali
5 Inf... 100 0 (0x640000) 3/23/2006 6:20:57 PM Denied: app
6 Inf... 100 0 (0x640000) 3/23/2006 6:21:21 PM Denied: app
7 Inf... 100 0 (0x640000) 3/23/2006 6:21:46 PM Denied: app
1: Information
Thursday, March 23, 2006 4:00:30 PM
Details:
Acronis Malicious Software Shield service is started.
Close

Log view window

Chapter 4. Using Acronis Malware Shield

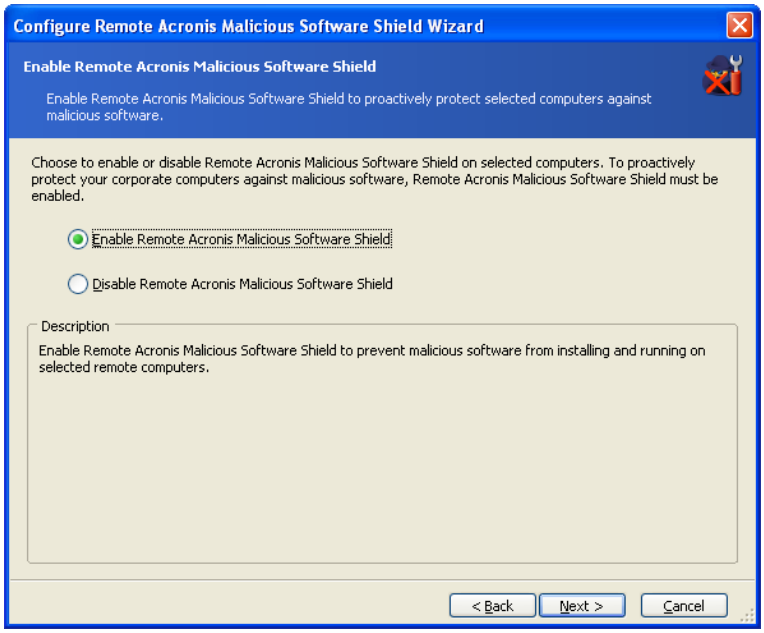
Acronis Privacy Expert Corporate not only enables you to remove malicious software from network computers, but it also prevents malware from accessing the user's PC. This function is provided by the Acronis Malware Shield — a special tool that monitors computer systems for suspicious applications and components.

4.1 Enabling Acronis Malware Shield

Malware Shield comes enable immediately after its installation (for more details about installation see *Chapter 1 Installing Acronis Privacy Expert Corporate components*). You can enable or disable it any time you want.

To enable or disable Acronis Malware Shield on the remote computers:

- Click the **Configure Malware Shield** button on the Toolbar or select **Tools → Configure Malware Shield** from the main menu. The **Configure Remote Acronis Malicious Software Shield Wizard** runs.
- In the **Select computers** window, select the network computers on which you want to enable or disable the Acronis Malware Shield
- In the next window, select **Enable** or **Disable** option.


Configure Remote Acronis Malicious Software Shield Wizard
Enable Remote Acronis Malicious Software Shield
Enable Remote Acronis Malicious Software Shield to proactively protect selected computers against malicious software.
Choose to enable or disable Remote Acronis Malicious Software Shield on selected computers. To proactively protect your corporate computers against malicious software, Remote Acronis Malicious Software Shield must be enabled.
Enable Remote Acronis Malicious Software Shield
Disable Remote Acronis Malicious Software Shield
Description
Enable Remote Acronis Malicious Software Shield to prevent malicious software from installing and running on selected remote computers.
< Back
Next >
Cancel

Malware Shield remote configuration window

To enable or disable Acronis Malware Shield on the local computer:

- Right-click the **Malware Shield** icon in the system tray

Copyright © Acronis, Inc., 2000-2006

- Select **Enable Acronis Malware Shield** or **Disable Acronis Malware Shield.**

A local computer user can remove the Malware Shield icon from the system tray by right-clicking the icon and selecting **Exit**. To show the Malware Shield icon again, select **Programs → Acronis → Malware Shield → Acronis Malware Shield.**

4.2 Setting up Malware Shield

A user can locally adjust the Malware Shield installed on his computer. To configure the Malware Shield settings on a local computer, right click on the **Acronis Malware Shield** icon in the system tray and select **Acronis Malware Shield Options**.

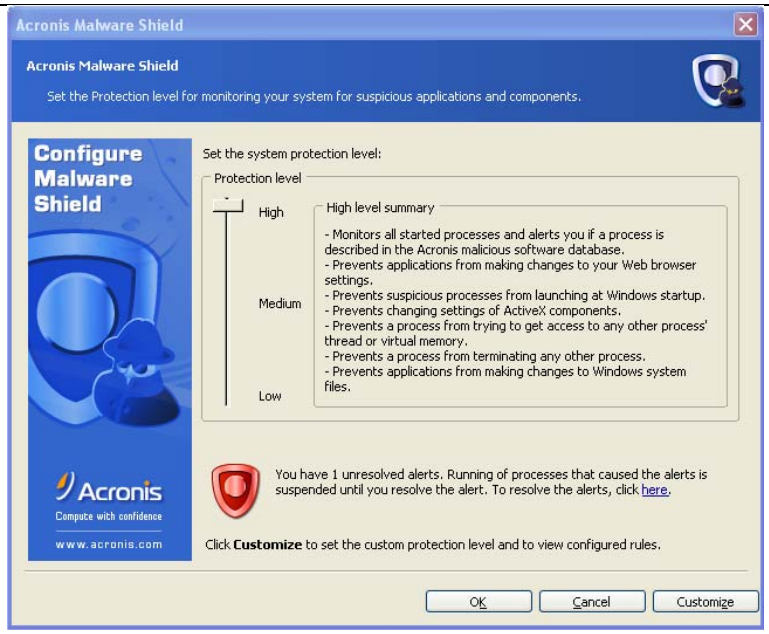
4.2.1 Setting up the system protection level

The **Protection Level** parameter defines the depth of monitoring the system for malicious software and applications.

- If the protection level is set to **Low**, the Shield monitors all running processes and alerts the user on detecting any process described in malicious software database.
- If the protection level is set to **Medium**, the Shield, in addition to monitoring processes, prevents suspicious processes from launching at Windows startup, prevents Web browser settings from hijacking and protects ActiveX components settings.
- The **High** protection level is most secure. It includes all Medium level precautions and also protects all processes and Windows system files against modification by other processes and applications. This setting might be recommended for experienced users.

Under Windows 9x operating systems the **High** protection level is not available because of OS limitations.

Copyright © Acronis, Inc., 2000-2006

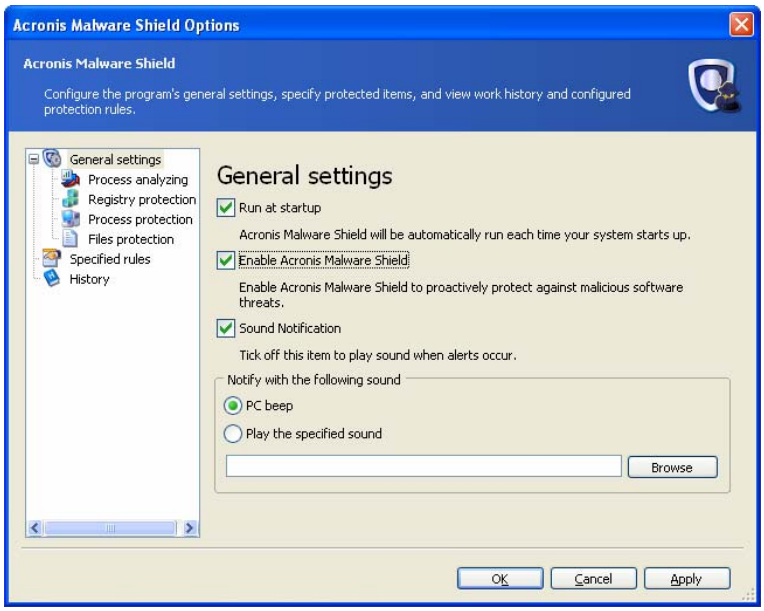

Acronis Malware Shield
Acronis Malware Shield
Set the Protection level for monitoring your system for suspicious applications and components.
Configure Malware Shield
Set the system protection level:
Protection level
High
Medium
Low
High level summary
- Monitors all started processes and alerts you if a process is described in the Acronis malicious software database.
- Prevents applications from making changes to your Web browser settings.
- Prevents suspicious processes from launching at Windows startup.
- Prevents changing settings of ActiveX components.
- Prevents a process from trying to get access to any other process' thread or virtual memory.
- Prevents a process from terminating any other process.
- Prevents applications from making changes to Windows system files.
Acronis
Compute with confidence
www.acronis.com
You have 1 unresolved alerts. Running of processes that caused the alerts is suspended until you resolve the alert. To resolve the alerts, click here.
Click Customize to set the custom protection level and to view configured rules.
OK
Cancel
Customize

System protection level

You can customize the selected protection level by adding options specific for the upper level or deleting options that you consider unnecessary. To view and/or customize options of the selected protection level click **Customize**.

4.2.2 General settings

In the **General settings** window, you can enable/disable Acronis Malware Shield and launching Acronis Malware Shield at system startup.


Acronis Malware Shield Options
Acronis Malware Shield
Configure the program's general settings, specify protected items, and view work history and configured protection rules.
General settings
Process analyzing
Registry protection
Process protection
Files protection
Specified rules
History
General settings
Run at startup
Acronis Malware Shield will be automatically run each time your system starts up.
Enable Acronis Malware Shield
Enable Acronis Malware Shield to proactively protect against malicious software threats.
Sound Notification
Tick off this item to play sound when alerts occur.
Notify with the following sound
PC beep
Play the specified sound
Browse
OK
Cancel
Apply

General settings window

If Acronis Malware Shield is enabled and **Run at startup** checked, the Shield will automatically launch at every operating system startup, show alerts and treat events according to user selections and rules.

Copyright © Acronis, Inc., 2000-2006

If Acronis Malware Shield is enabled and **Run at startup** not checked, the Shield will not function after system startup. To start the Shield, select **Programs → Acronis → Malware Shield → Acronis Malware Shield.**

If Acronis Malware Shield is disabled and **Run at startup** checked, the Shield will launch at system startup but its protection functions will not work. You will be able to adjust and enable Acronis Malware Shield using its icon in the System Tray.

If Acronis Malware Shield is disabled and **Run at startup** not checked, the Shield will not function after system startup. To make the Shield to operate, select **Programs → Acronis → Malware Shield → Acronis Malware Shield** and enable the Shield using its icon in the System tray.

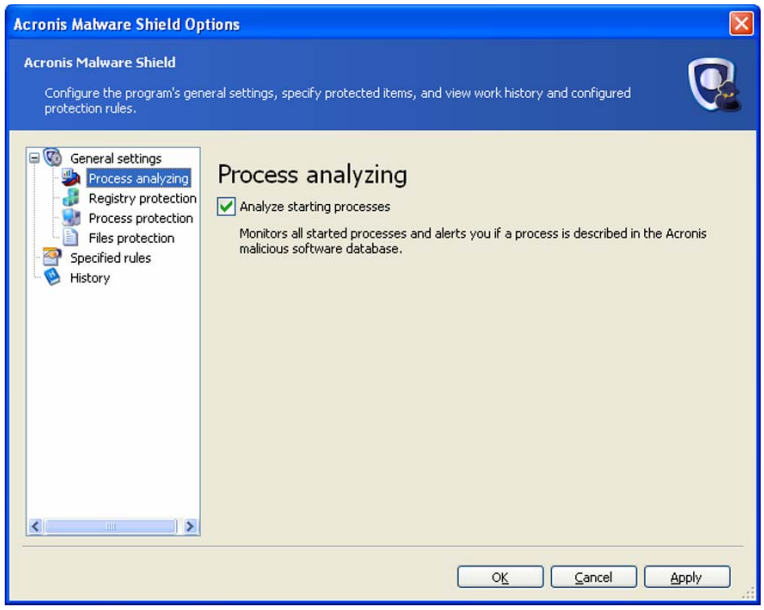
You may also want to enable **Sound Notification** (PC beep or playing the specified melody in WAV format) in addition to displaying alert windows.

Having set up all settings, apply changes by clicking **Apply** button.

Use **Cancel** button if you do not want changes to be applied.

4.2.3 Process analyzing

Tick off **Analyze starting processes** to enable the Shield monitor all starting processes and alert the user on detecting any process described in malicious software database.



Process analyzing

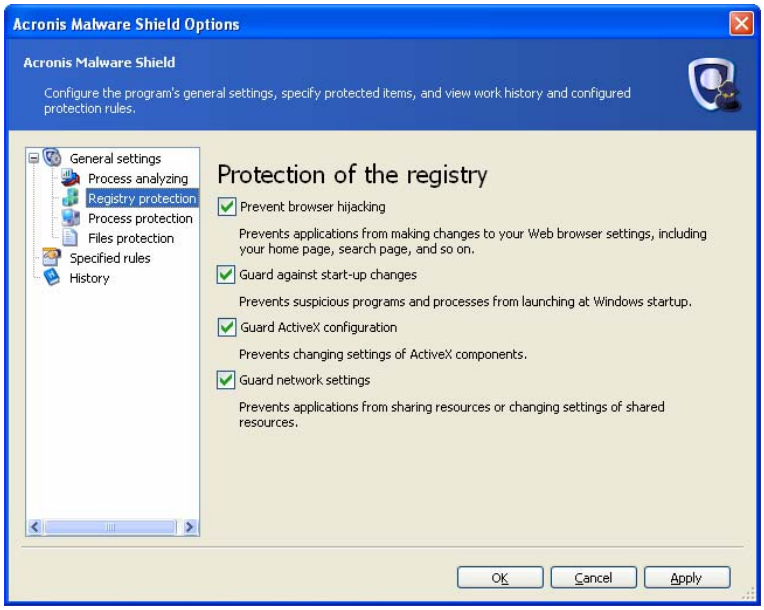
4.2.4 Registry protection

In the **Registry protection** section, you can enable/disable:

- Browser settings protection from hijacking by suspicious applications (for example, changing the home page)

Copyright © Acronis, Inc., 2000-2006

- Preventing suspicious software and processes from launching at system startup
- Protection of the ActiveX components settings
- Preventing application from sharing resources or changing settings of shared resources


Acronis Malware Shield Options
Acronis Malware Shield
Configure the program's general settings, specify protected items, and view work history and configured protection rules.
General settings
Process analyzing
Registry protection
Process protection
Files protection
Specified rules
History
Protection of the registry
Prevent browser hijacking
Prevents applications from making changes to your Web browser settings, including your home page, search page, and so on.
Guard against start-up changes
Prevents suspicious programs and processes from launching at Windows startup.
Guard ActiveX configuration
Prevents changing settings of ActiveX components.
Guard network settings
Prevents applications from sharing resources or changing settings of shared resources.
OK
Cancel
Apply

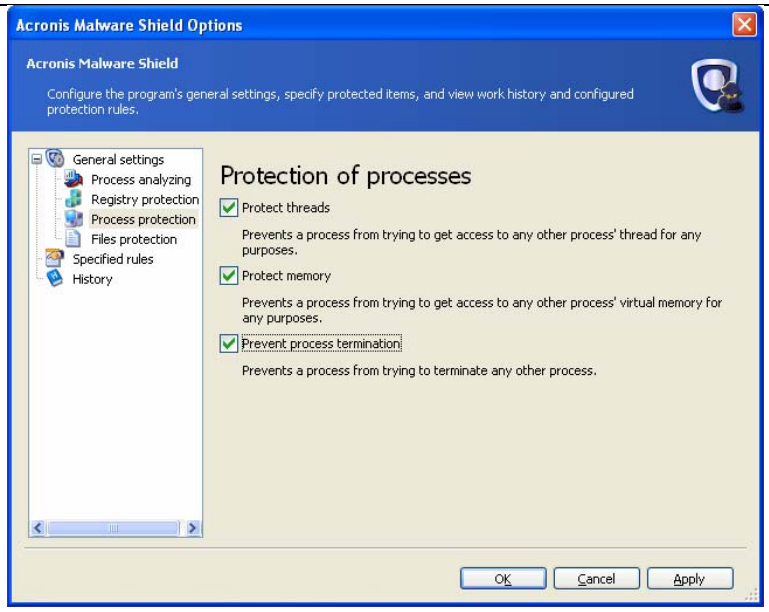
Registry protection

4.2.5 Process protection

In the **Process protection** section, you can prohibit or allow all running processes to perform the following actions:

- Access to other processes threads
- Access to other processes virtual memory
- Terminate other processes.

 Copyright © Acronis, Inc., 2000-2006


Acronis Malware Shield Options
Acronis Malware Shield
Configure the program's general settings, specify protected items, and view work history and configured protection rules.
General settings
Process analyzing
Registry protection
Process protection
Files protection
Specified rules
History
Protection of processes
Protect threads
Prevents a process from trying to get access to any other process' thread for any purposes.
Protect memory
Prevents a process from trying to get access to any other process' virtual memory for any purposes.
Prevent process termination
Prevents a process from trying to terminate any other process.
OK
Cancel
Apply

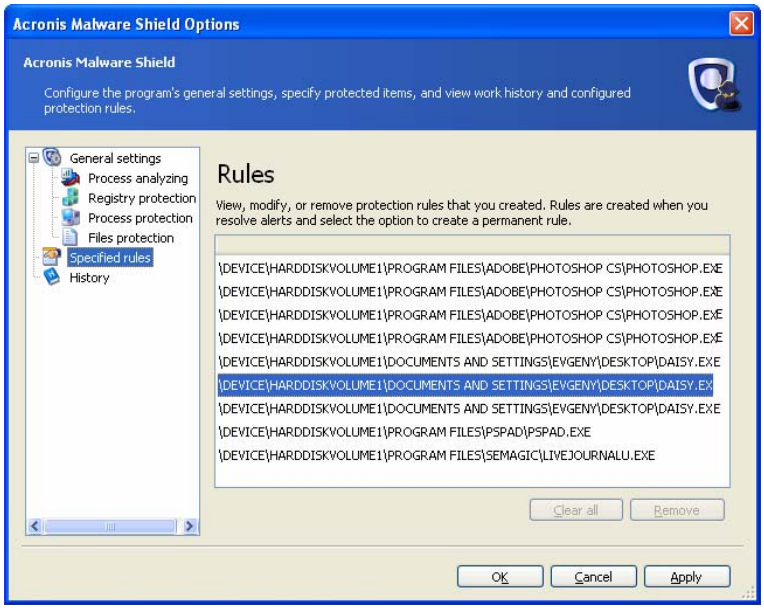
Process protection

4.2.6 Files protection

In the **Files protection** section, you can enable/disable protection of your system files, critical to Windows operation, from changing by applications.

4.2.7 Specified rules

The **Specified rules** section contains a list of protection rules specified by the user in the alerts window (see *4.3 Handling the Malware Shield Alerts*). You can remove the selected rule by clicking **Remove** or use **Clear all** to remove all entries.

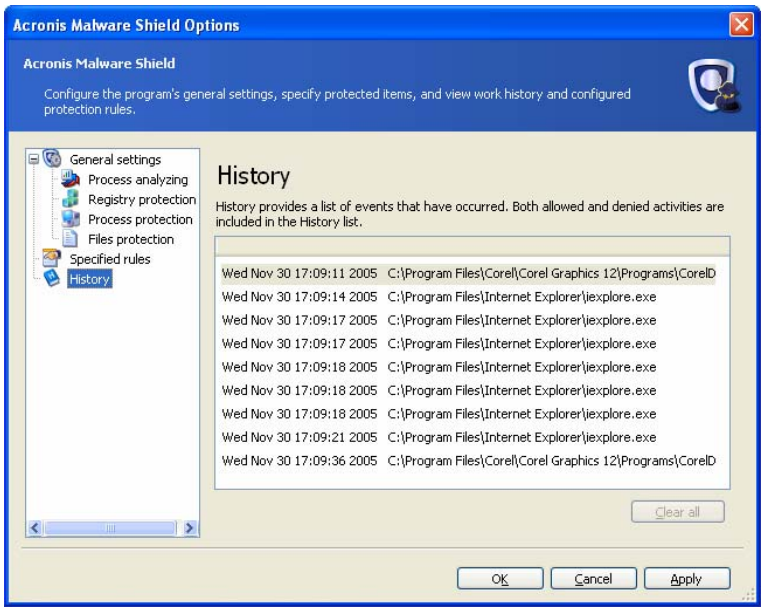


Specified rules

Copyright © Acronis, Inc., 2000-2006

4.2.8 History

The **History** section contents a list of all events occurred, so you can view and analyze it. Use **Clear all** button to remove all list entries.


Acronis Malware Shield Options
Acronis Malware Shield
Configure the program's general settings, specify protected items, and view work history and configured protection rules.
General settings
Process analyzing
Registry protection
Process protection
Files protection
Specified rules
History
History
History provides a list of events that have occurred. Both allowed and denied activities are included in the History list.
Wed Nov 30 17:09:11 2005 C:\Program Files\Corel\Corel Graphics 12\Programs\CorelD
Wed Nov 30 17:09:14 2005 C:\Program Files\Internet Explorer\iexplore.exe
Wed Nov 30 17:09:17 2005 C:\Program Files\Internet Explorer\iexplore.exe
Wed Nov 30 17:09:17 2005 C:\Program Files\Internet Explorer\iexplore.exe
Wed Nov 30 17:09:18 2005 C:\Program Files\Internet Explorer\iexplore.exe
Wed Nov 30 17:09:18 2005 C:\Program Files\Internet Explorer\iexplore.exe
Wed Nov 30 17:09:18 2005 C:\Program Files\Internet Explorer\iexplore.exe
Wed Nov 30 17:09:21 2005 C:\Program Files\Internet Explorer\iexplore.exe
Wed Nov 30 17:09:36 2005 C:\Program Files\Corel\Corel Graphics 12\Programs\CorelD
Clear all
OK
Cancel
Apply

History window

4.2.9 Saving settings for Acronis Malware Shield

Having set up Acronis Malware Shield, click **OK** if everything is correct.

All Malware Shield settings will be active until you change them again in the same way.

4.3 Handling the Malware Shield Alerts

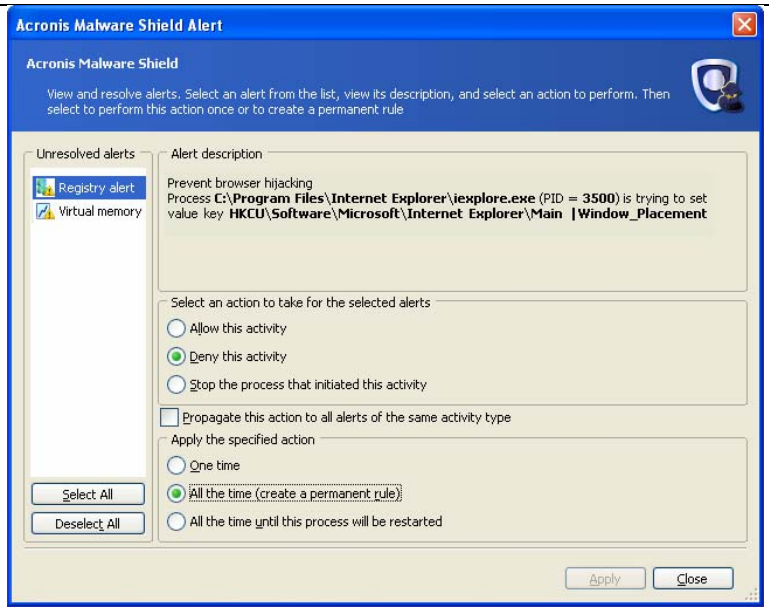
When a suspicious event is detected, the Acronis Malware Shield icon in the system tray starts to blink. To open the alerts window double click on the Malware Shield icon.

Then select an unresolved alert (or group of alerts), read its description and choose an action to be taken: allow or deny the activity that caused the alert, or stop the process that initiated this activity.

To extend the chosen action to all other alerts of the same activity type check the **Propagate this action to all alerts of the same activity type** parameter.

You should also choose how to apply the specified action: **One time**, **All the time (create a permanent rule)** or **All the time until this process will be restarted**.

Copyright © Acronis, Inc., 2000-2006


Acronis Malware Shield Alert
Acronis Malware Shield
View and resolve alerts. Select an alert from the list, view its description, and select an action to perform. Then select to perform this action once or to create a permanent rule
Unresolved alerts
Registry alert
Virtual memory
Alert description
Prevent browser hijacking
Process C:\Program Files\Internet Explorer\iexplore.exe (PID = 3500) is trying to set value key HKCU\Software\Microsoft\Internet Explorer\Main |Window_Placement
Select an action to take for the selected alerts
Allow this activity
Deny this activity
Stop the process that initiated this activity
Propagate this action to all alerts of the same activity type
Apply the specified action
One time
All the time (create a permanent rule)
All the time until this process will be restarted
Select All
Deselect All
Apply
Close

Alert window

If you choose to **Close** the alerts window, no actions will be taken. The Malware Shield icon in the system tray will continue blinking, notifying that you have unresolved alerts.

Copyright © Acronis, Inc., 2000-2006

Chapter 5. Malware definitions updates

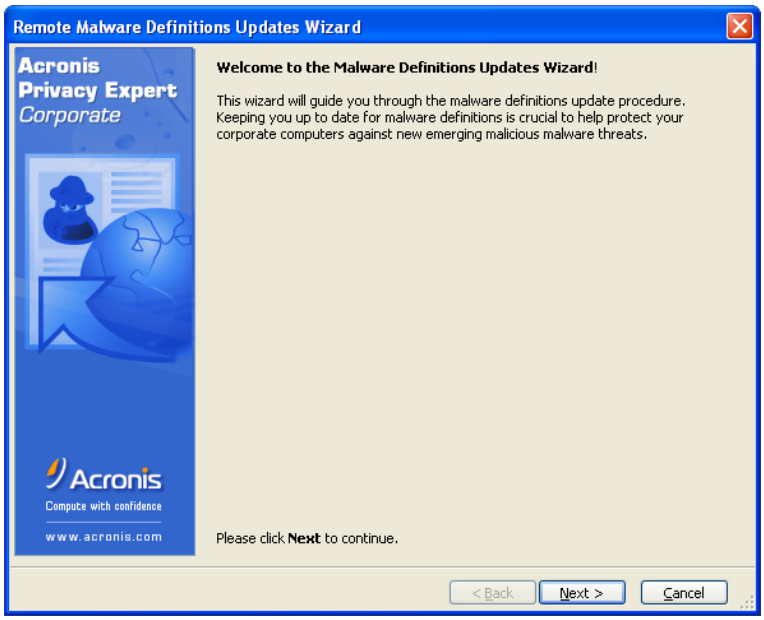
Offering you timely and reliable protection from new malware released as often as every day, Acronis Privacy Expert Corporate maintains the special **Malware definitions updates** service. It enables users to obtain the most up-to-date information and malware protection from Acronis website.

5.1 Malware database update

5.1.1 Running Malware Definitions Updates Wizard

You can run the **Malware Definitions Updates Wizard** in the Acronis Privacy Expert Corporate Management Console main window the following ways:

- By selecting **Tools** → **Web updates** in the menu
- By clicking **Web updates** on the toolbar.

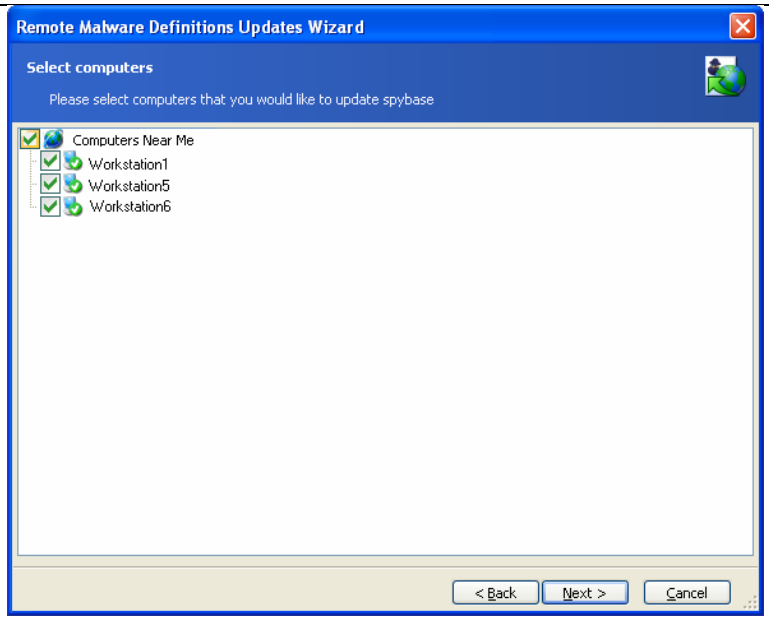

Remote Malware Definitions Updates Wizard
Acronis
Privacy Expert
Corporate
Welcome to the Malware Definitions Updates Wizard!
This wizard will guide you through the malware definitions update procedure. Keeping you up to date for malware definitions is crucial to help protect your corporate computers against new emerging malicious malware threats.
Acronis
Compute with confidence
www.acronis.com
Please click Next to continue.
< Back
Next >
Cancel

Malware definitions update wizard

5.1.2 Selecting remote computers to update malware definitions

Next, select the remote computers on which you are going to update malware definitions.

Copyright © Acronis, Inc., 2000-2006

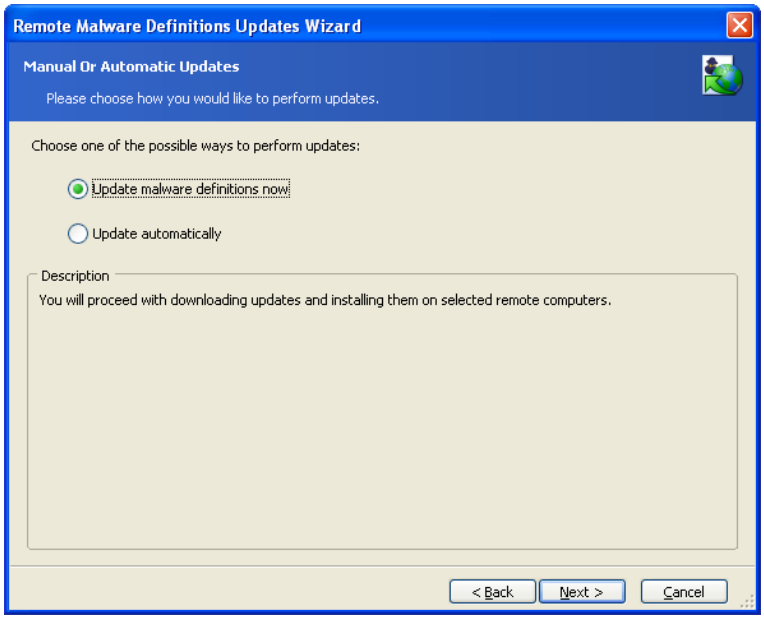


Select computers window

5.1.3 Selecting update mode

Select the update mode: either manual or scheduled automatic:

- To update malware definitions **right now**, select **Update malware definitions now**
- To **automatically update** malware definitions on a schedule, select **Update automatically**.


Remote Malware Definitions Updates Wizard
Manual Or Automatic Updates
Please choose how you would like to perform updates.
Choose one of the possible ways to perform updates:
Update malware definitions now
Update automatically
Description
You will proceed with downloading updates and installing them on selected remote computers.
< Back
Next >
Cancel

Selecting update mode window

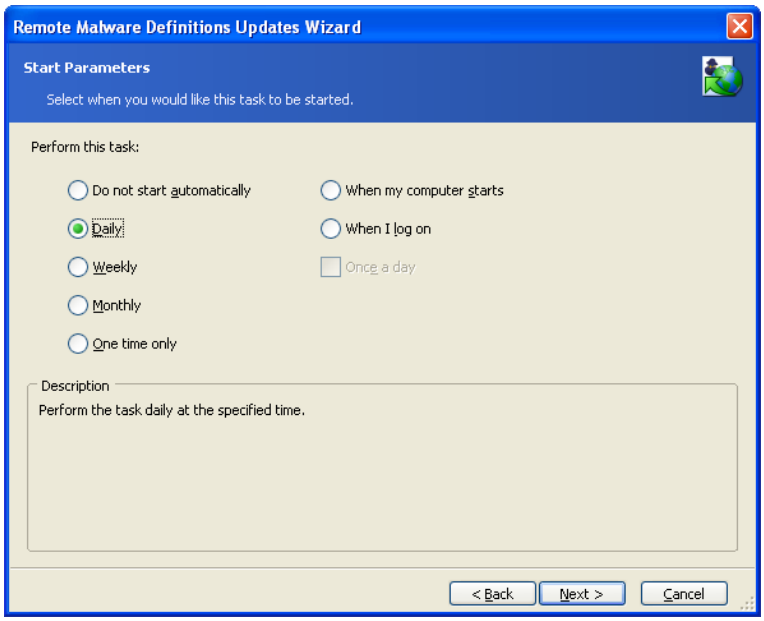
5.1.4 Setting the schedule

If you select automatic updates, you will be asked to set the update schedule.

Copyright © Acronis, Inc., 2000-2006

The following variants are available:

- **Daily**, according to the schedule with the ability to select only workdays or once every few days
- **Weekly**, according to the schedule with the ability to select particular days, such as Tuesday and Friday, or once every two or three weeks, etc
- **Monthly,** according to the schedule on the time and day set; The suite supports clean-up on the <first, second, third, fourth, last> <day of the week> (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday), for example
- **One time only,** at a specific time (hours:minutes) on a particular day (month/day/year)
- **When my computer starts** (you may specify launching the task once a day only)
- **When I log on** (you may specify launching the task once a day only)



Set the update schedule

Having made a selection, click **Next** to set additional parameters on the next wizard page.

5.1.5 Entering user name and password

To finish scheduling automatic updates, enter the user name and password for access to the remote computers. See details in 3.4.4.

Copyright © Acronis, Inc., 2000-2006

Chapter 6. Acronis Pop-up Blocker

6.1 What are pop-ups?

While browsing some Web sites, you might have unwanted pop-up windows open along with the window you want. Generally, pop-ups contain bothersome advertising. They decrease your Internet connection speed and increase the traffic you pay for. On some Web sites, pop-ups are used to provide extra information or forms for filling up by users.

6.2 Acronis Pop-up Blocker

Acronis Pop-up Blocker automatically comes enable during installation and prevents Microsoft Internet Explorer windows from opening, except the ones the user wants to view. User can set up filters for various kinds of web pages contents (GIF files and flash animation, ActiveX objects, pop-ups in layers, etc.).

Acronis Pop-up Blocker may be installed locally or remotely using the Acronis Privacy Expert Corporate Management Console (See section *1.7 Installing Acronis components onto remote machines* of this Guide).

After that, the local user can disable/enable the Acronis Pop-up Blocker or change its options.

A local computer user can remove the Acronis Pop-up Blocker icon from the system tray by right-clicking the icon and selecting **Exit**. To show the Pop-up Blocker icon again, select **Programs → Acronis → Pop-up Blocker → Acronis Pop-up Blocker.**

6.3 Acronis Pop-up Blocker options

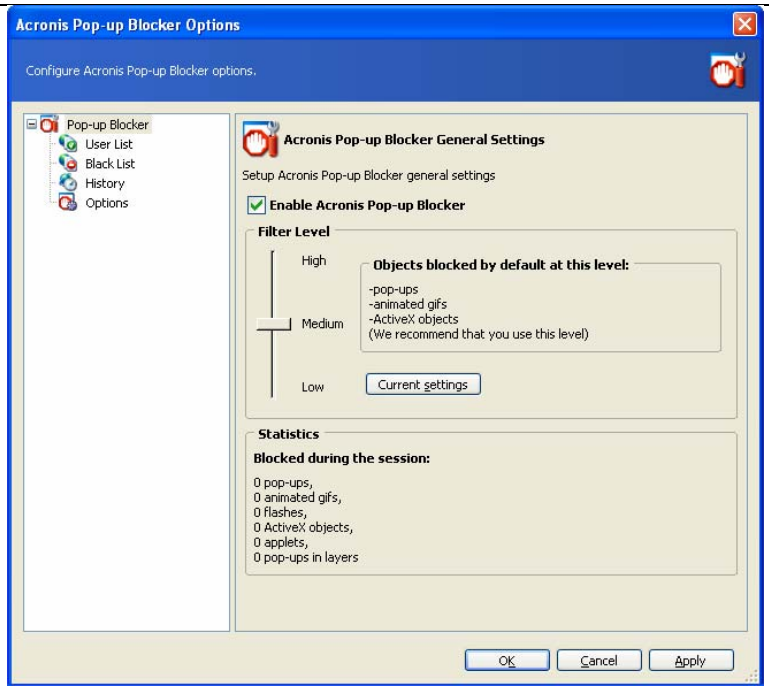
You can invoke the Acronis Pop-up Blocker options window in the following ways:

- By selecting **Acronis Pop-up Blocker** in the **Tools** menu of the Internet Explorer
- By clicking **Acronis Pop-up Blocker** icon on the toolbar of the Internet Explorer
- By right-clicking on a web page and selecting **Acronis Pop-up Blocker – Options** on the context menu

6.3.1 Acronis Pop-up Blocker General Settings

In the general settings section you can enable or disable Acronis Pop-up Blocker and choose the appropriate filter level (types of web page content that will be blocked).

Copyright © Acronis, Inc., 2000-2006



Pop-up Blocker settings

- **Low** filter level means blocking pop-ups only.
- If the filter level is set to **Medium**, the Pop-up Blocker, in addition to blocking pop-ups, prevents display of animated GIF files and blocks ActiveX objects.
- The **High** protection level (recommended) includes all Medium level precautions and also bans flash animation, applets and pop-ups in layers.

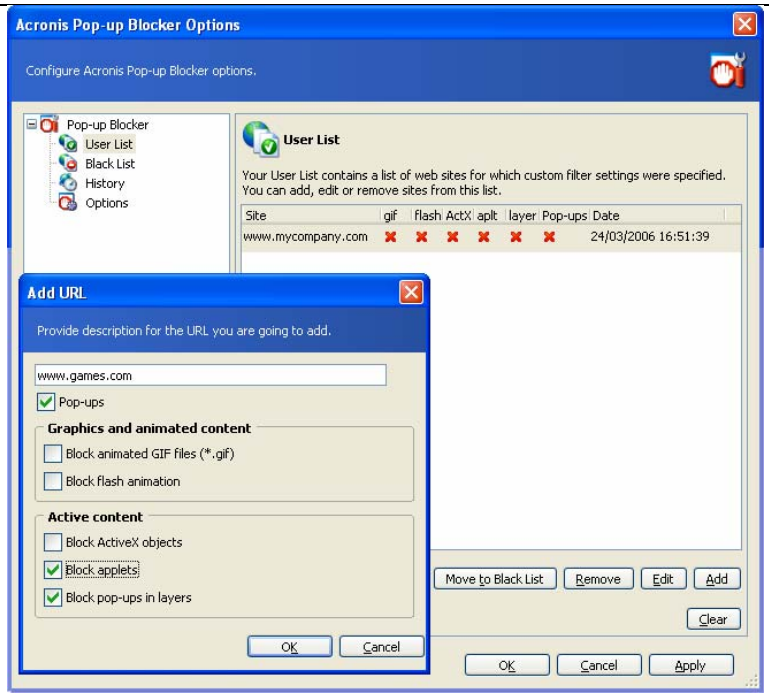
You can create your own set of filter options by clicking **Current settings** and selecting types of contents to be blocked. User's set of options has priority over the selected filter level. Therefore, the filter level slider may change position after **Current settings** modification.

At the bottom of the window Acronis Pop-up Blocker displays statistics of the objects, blocked during the current session.

6.3.2 User List

If you want to set individual filtration rules for any site, add this site to **User List**.

 Copyright © Acronis, Inc., 2000-2006



User list

To manually add a site to the **User List**, click the **Add** button, enter the site URL and adjust filter settings.

Acronis Pop-up Blocker automatically generates entries for the **User List** while the user explores Internet (see *6.3.4 History*). To apply these entries, simply move them to the **User List**.

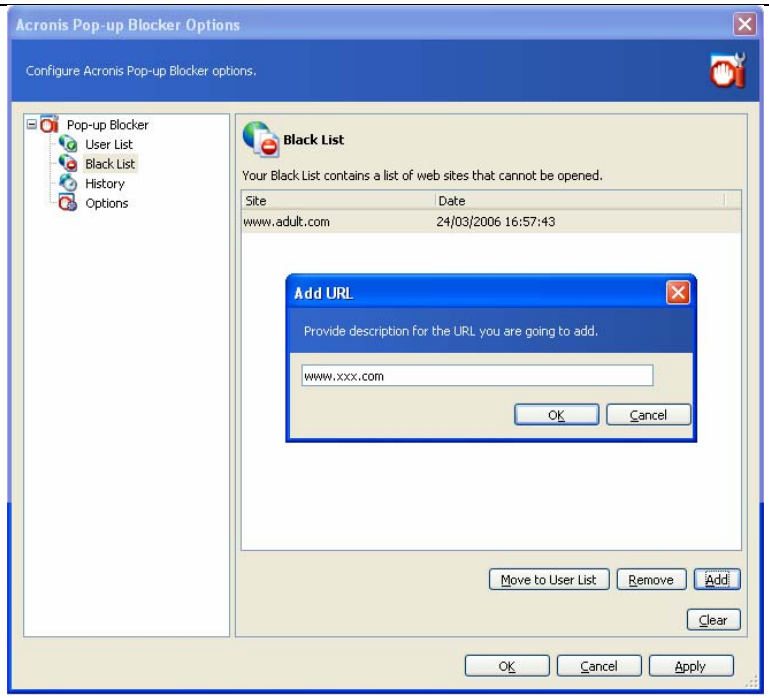
To edit the existing filter settings select the site, click the **Edit** button and make the necessary changes in the appearing window.

You can also move, if need be, any site from **User List** to the **Black list** to forbid visiting this site at all. The **Remove** button rejects the selected site from the list. To remove all entries from the list, use **Clear** button.

6.3.3 Black List

Adding a site to the **Black list** means that Acronis Pop-up Blocker will prevent following any link to this site, and show a report in IE status bar (if enabled): "Acronis Pop-up Blocker: this link is from the Black URL list – navigation was stopped!". Use this option to prevent automatic switching to certain URLs that may be initiated by some web pages.

Copyright © Acronis, Inc., 2000-2006



Black list

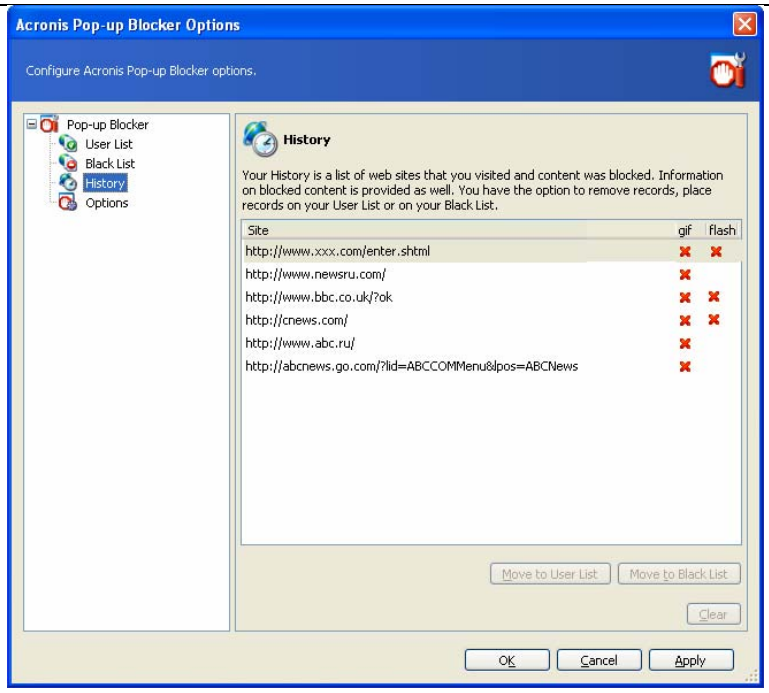
To add a site to the **Black List**, click the **Add** button and enter the site URL. Also you can move any site from other lists to the **Black list** by clicking **Move to Black List**.

To remove a site from the list click **Remove**. To remove all entries from the list, use **Clear** button.

6.3.4 History

The **History** section contains a list of visited websites where any kind of contents was blocked and information about the types of the blocked content. In fact, this information is a ready filter, that has been automatically set by Acronis Pop-up Blocker, for every listed site.

 Copyright © Acronis, Inc., 2000-2006



History

If you move a site from **History** to **User List**, at next visiting this site the program will block the same type of contents as it blocked before.

Leaving a site in **History** is equal to no special filter settings for this site. Next time Acronis Pop-up Blocker will filter its contents according to the common rules.

You can also move, if need be, any site from **History** to the **Black list** to forbid visiting this site at all. To remove all entries from the list, use **Clear** button.

6.3.5 Acronis Pop-up Blocker options

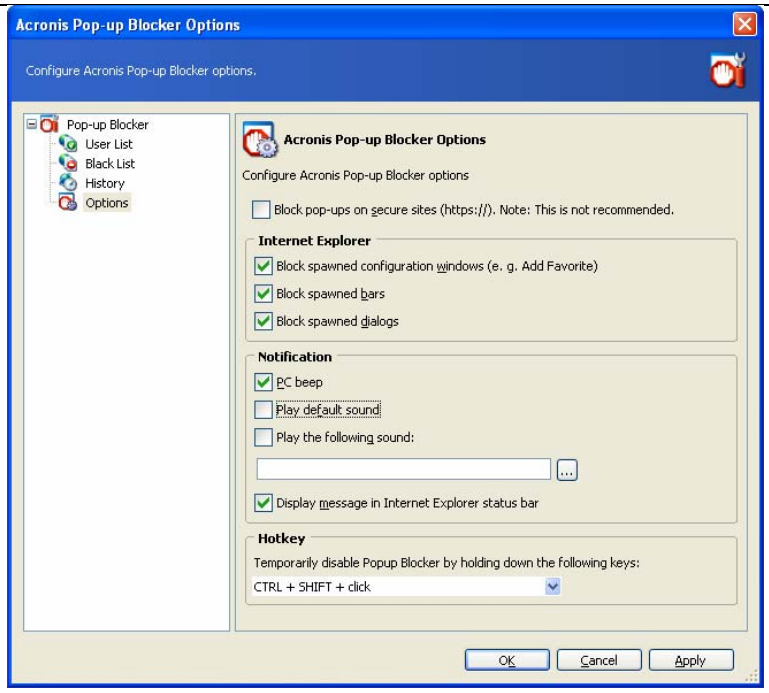
In this section you can, if need be, enable additional Acronis Pop-up Blocker protection options:

- Blocking pop-ups on secure sites (transferred via https protocol). Enable https blocking only if it is really necessary!
- Blocking the Internet Explorer spawned configuration windows, dialogs and panels (for example, an Add Favorite window that annoyingly suggests to add the current page to Favorites list)

This window also allows you:

- set up/disable sound notification at blocking web pages contents (PC beep, play default sound, select sound);
- enable/disable notification in the Internet Explorer status bar;
- specify hotkeys for temporary disabling Acronis Pop-up Blocker.

Copyright © Acronis, Inc., 2000-2006



Options

Copyright © Acronis, Inc., 2000-2006

Appendix A. Malware threats glossary

This glossary contains supplemental information on the most popular malware from which Acronis Privacy Expert Corporate protects your organization computers.

Adware

This is a kind of Web marketing where banners are integrated into freeware and shareware programs. To be able to use a program, a user has to watch ads downloaded from the Web. This increases traffic volume and slows down your Internet connection.

Backdoors

Backdoor allows the malefactor to secretly control a remote computer: copy files, run programs, edit registry, reboot, change passwords etc. Backdoors may be used for attacking other computers via the infected computer thus hiding the real attacker location.

Browser Helper Objects

Some Browser Helper Objects are useful at expanding your browser's capabilities, but there are others that might not need your permission to install on your computer and that can be used for malicious purposes, such as gathering information on your Web surfing habits. This can cause problems ranging from incompatibility issues to corrupting important system functions, making these objects not only a threat to your security, but also to your system's stability.

Browser hijackers

Browser hijackers have the ability to change your Internet browser settings, redirect your Web searches through their own search engines, redirect mistyped or incomplete URLs, and change your default home page. They can redirect your searches to "pay-per-search" Web sites or pornographic Web sites.

Commercial keylogger

Keyloggers register which keys are pressed on a user's PC and transmit this information via e-mail. Such applications can also store the time of running or quitting any applications. They can operate without the users' knowledge.

Dialers

Dialers have the ability to disconnect your computer from your local Internet provider and reconnect you to the Internet using an alternate connection, such as an expensive pornographic, toll or international phone number. They do not

Copyright © Acronis, Inc., 2000-2006

spy on you but they can rack up significant long-distance phone charges. They have the ability to run in the background, hiding their presence.

Exploit/Security holes

These are security bugs and vulnerabilities in applications primarily meant for Web operations. Through such holes, intruders can corrupt a PC or gain remote control over it.

Remote Administration

This is a kind of software, including commercial software, designed for remote PC control. In some cases, users might not be aware of such applications running.

Rootkits

RootKit is a program capable to intercept and modify low-level system functions (API) in order to mask its presence in the system. Different kinds of malware, especially trojans and backdoors, use rootkit technology for making invisible processes, services, registry keys, files and folders created by these programs.

Sniffers

Sniffers are programs that capture network traffic (sent and received data packets). Sniffers can be a serious threat, able to capture and decrypt user names, passwords and private information and prevent normal operation of computers and networks in general. As most protocols (FTP, POP, HTTP, telnet) have secret information transmitted unencrypted, an intruder can easily gain access to a user's information by setting up sniffer filters and waiting for the victim to connect to a server.

Spyware

Spyware are programs that secretly gather and transmit personal user information. Spyware can be a part of various applications, including commercial products.

Toolbars

Toolbars can be downloaded to your Web browser to make browsing easier. Examples include the Google, Alexa and Yahoo toolbars. Even though these are very handy to use, they have the ability to track everything you do on the Internet and to pass that information back to the owners of the toolbars. Be sure to read the terms and conditions page before you download any toolbar.

 Copyright © Acronis, Inc., 2000-2006

Trojan Horses (Trojans)

Trojans are specially created programs that are deployed to PCs imitating useful applications and utilities. They can result in failures, lock-ups or even complete data destruction. Trojans are spread via mailing lists, Web forums, etc.

Copyright © Acronis, Inc., 2000-2006